Small Business Telecom & Computing

LIBERTY-BELL

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

EB Docket 06-TC-060

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 29, 2008

Liberty Bell Telecom

Form 499 Filer ID: 824050

Name of signatory: Jay Weber

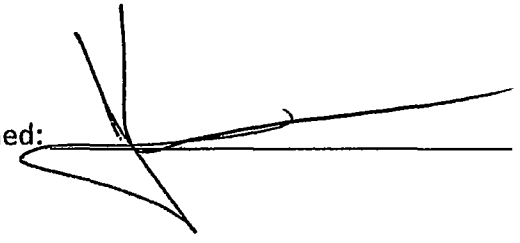
Title of signatory: President

I, Jay Weber, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken any actions (proceedings instituted or petitions filed by a Company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI , and what steps Companies are taking to protect CPNI.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a Company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed: 

Small Business Telecom & Computing

LIBERTY-BELL

Statement Concerning the Protection of Customer Proprietary Network Information for the Annual Period Ending December 31, 2007

1. Liberty Bell Telecom ("Company") is a telecommunications carrier subject to the requirements set forth in Section 64.2009 of the Federal Communications Commission's ("FCC's") rules. Company has established policies and procedures to satisfy compliance with the FCC's rules pertaining to use, disclosure and access to customer proprietary network information ("CPNI") set forth in sections 64.201 et. seq.

2. If a customer calls Company requesting information that is considered CPNI, Company does not release such information unless customer provides a pre-established password, requests that the information be sent to the customer's address of record, or Company calls the telephone number of record and discusses the requested information.

3. Without customer approval, Company does not use, disclose or permit access to CPNI to provide or market service offerings within a category of service to which the customer does not already subscribe, except as permitted by the FCC rules.

4. Information protected by Company includes information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by a customer and made available to Company by the customer solely by virtue of the carrier-customer relationship. Also protected is information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer.

5. Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

6. Company has established a system by which they can determine whether a customer has approved or disapproved of Company's release or use of CPNI prior to that information being used or released.

7. Company personnel are trained as to when they are and are not authorized to release or use CPNI, and violation of these rules will subject personnel to express disciplinary action.

8. If and when customer approval to use, disclose, or permit access to customer CPNI is desired, Company obtains such customer approval through written or oral methods (however, we only utilize the oral authorization to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts, and such CPNI authority, if granted, lasts only for the duration of that specific call). Company honors a customer's approval or disapproval until the customer revokes or limits such approval or disapproval.

9. Company has established a procedure whereby all sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval of the use of CPNI and records reflecting carrier compliance with the Commission Rules are maintained for a minimum of one year.

10. Prior to any solicitation for customer approval, Company provides notification to customers of their right to restrict use of, or disclosure of, and access to the customer's CPNI. Records of these notifications are maintained for a period of at least one year.

11. Company's notifications provide information sufficient to enable our customers to make informed decisions as to whether to permit the use or disclosure of, or access to, their CPNI. Company's notifications do: (1) contain a statement that the customer has a right, and Company has a duty under federal law, to protect the confidentiality of CPNI; (2) specify the types of information that constitute CPNI and the specific entities that will receive the CPNI; (3) describe the purposes for which the CPNI may be used; and (4) inform the customer of the right to disapprove those uses and deny or withdraw access to or use of CPNI at any time.

12. Company's notifications inform the customer that any approval or denial of approval for the use of CPNI outside of the service to which the customer already subscribes is valid until the customer affirmatively revokes or limits such approval or denial.

13. Company advises its customers of the precise steps the customer must take in order to grant or deny access to CPNI, and that denial of approval will not affect the provision of any services to which the customer subscribes.

14. Company maintains a record of its sales and marketing campaigns that use customer's CPNI. Further, a record of all instances where CPNI was disclosed or provided to third parties or where third parties were allowed access to CPNI is maintained by Company. These records reflect a description of the campaigns, the specific CPNI used in the campaign and what products or services were offered as part of the campaign. These records are retained for a minimum of one year.

15. Company obtains opt-in consent from customers before disclosing customer's CPNI to any joint venture partner or independent contractor.

16. If a breach of CPNI occurs, Company will provide electronic notification of the breach to the U.S. Secret Service and the FBI within seven (7) days. Company will also notify customer after seven (7) more days unless there is a risk of immediate and irreparable harm to the customer in which case Company will notify the customer immediately. Company will keep records or discovered breaches for at least two (2) years.

17. Liberty Bell Telecom does not release any information to third parties, unless required to do so by court order.

18. Liberty Bell Telecom does collect Customer Proprietary Information at the time of account inception.

19. Liberty Bell Telecom obtains customer information via our online order management system. (Operated by BeQuick Software Inc. 7108 Fairway Dr., Suite 260, Palm Beach Gardens, FL 33418)

20. In addition to collecting information via our online order management system, we also gather necessary customer information over the phone as well as on customer order forms (applications for telecommunications services).

21. Telephone communications with customers are not recorded unless authorized by the customer. Telephone conversations that are recorded are stored on a remote server that is located in a secured facility. Access to recorded conversations is via user name and password, over a 128bit encrypted web connection.

22. Persons calling into our support center are required to verify account specific information, before a representative will disclose account information. Additionally Liberty Bell Telecom offers customers the ability to password protect their accounts.

23. Applications for service are stored in secured file cabinets in a secured room only accessible by authorized employees of Liberty Bell Telecom. Liberty Bell Telecoms customer support facility is a secured access facility and not open to the public.

24. All other customer information is stored electronically in our customer management system QuickTel. (Operated by BeQuick Software Inc.) QuickTel is a client application that is installed on our local systems. Access to the QuickTel application is limited to Liberty Bell Telecom Employees and Contractors. Access to QuickTel is protected by user name and password security, additionally management limits users access rights by login.

25. Liberty Bell Telecom and BeQuick Software, use off site servers, which are located in secure facilities only accessible by technicians with access cards. Liberty Bell Telecom also has on site servers which are secured. All electronic data transmissions between servers are encrypted at 128bits. Firewalls are also present at all locations to prevent intrusion.

26. Credit card payments are processed via Verisign, using SGC-enabled SSL certificates with a minimum of 128bit encryption.

27. Liberty Bell Telecom uses a payment processing center to process paper payments; the payment-processing center provides Liberty Bell Telecom with a batch upload file that does not contain any customer proprietary information. Employees of the payment-processing center receive payments via a lockbox. All employees of the payment-processing center are background checked and not allowed to take any information out of the center with them.

28. Paper payments are sent to our financial institution via bonded and insured carriers. Paper payments received directly by Liberty Bell Telecom are processed by employees, entered into our system, then stored in a lock box until picked up by a bonded and insured carrier and taken to our financial institution. All payments are secured during transport and only accessible by a bank representative.

29. Liberty Bell Telecom sends out paper invoices on a monthly basis to customers. A vendor that is located in a secure facility not accessible to the public prints bills. All employees of the vendor are background checked. The vendor receives billing information via batch files over a 128bit encrypted Internet connection. Batch files are stored on a secured server that is fire walled and password protected.

30. Customer data is often archived by Liberty Bell Telecom and its affiliates, archived information is stored on mass media and kept in secured facilities. Archived information is only available to authorized company personal.

31. Liberty Bell Telecom provides access to customers via an on line account manager. The account manager is protected via user name and password established by the customer. At the time the customer creates and on line profile, account information is verified. All data transmitted between the customer and the on line account manager is via a 128bit encrypted connection. The online account manager is a function of QuickTel and is governed by the same security policies as mentioned above.

32. Liberty Bell Telecom only uses customer information when necessary, and informs customers when it intends to do so, Customers sign a letter of authorization which informs the customer of when such information will be released and for what purpose.

33. Liberty Bell Telecom does not use customer information for marketing. Liberty Bell Telecom sends out non-customer specific advertisements in bill inserts. Liberty Bell Telecom also advertises via mass media outlets such as radio and television. Liberty Bell Telecom also periodically sends out direct mail advertisements, with lists provided by print vendors.

34. Liberty Bell uses customer information to determine credit worthiness and to order services from the ILEC. Liberty Bell obtains credit information from customers via Equifax, via a Verisign secured website that is user name and password protected. Only authorized employees of Liberty Bell Telecom have access to the credit system and access is monitored and controlled by management.

35. Credit checks and denials are processed in accordance with state and federal laws.

36. Liberty Bell Telecom orders services via a secured application secured at 128bits provided by the ILEC (Qwest). The application is user name and password protected, Qwest and Liberty Bell Telecom control access.

37. Liberty Bell Telecom cannot speak to Qwests policies regarding customer information. Liberty Bell Telecom does request that customers be excluded from marketing lists when submitting orders. Liberty Bell Telecom also requests that customer's information is not provided to non essential personal or any third party vendors.